WHAT IS CLAIMED IS:

1. A security policy database cache comprises:

at least one primary table including signature values that indicate that a IPSec packet's security policy database (SPD) information may be in the cache; and

at least one secondary table including cache entries having a selector, flags, security association (SA) information and an operation to perform on the corresponding packet for which a cache lookup was made.

2. The security policy database cache of claim 1 wherein the at least one primary table resides in DRAM.

3. The security policy database cache of claim 1 wherein the at least one secondary table resides in SDRAM.

4. The security policy database cache of claim 1 wherein at least one primary table and the at least one secondary table resides in the same memory.

5. The security policy database cache of claim 1 wherein the at least one primary table and the at least on secondary table resides in shared memory accessible by engines of a network processor.

6. The security policy database cache of claim 1 wherein the at least one primary table is divided into a plurality of buckets and each bucket is subdivided into bins.

7. The security policy database cache of claim 1 wherein the cache has a one-to-one correlation between the at

least one primary table location and the at least one secondary table.

8. The security policy database cache of claim 1 wherein the signature index for the first primary table is produced using an IP selector and either a hardware hash unit or a software hashing algorithm.

9. The security policy database cache of claim 8 wherein the IP selector can be either IPv4 or IPv6 and includes IP destination, IP source, IP protocol, IP source port, IP destination port.

10. The security policy database cache of claim 10 wherein when the at least one primary table is searched for a matching signature to a packet, and if no matching signature is found, the at least one secondary table is not accessed.

11. The security policy database cache of claim 10 wherein when the at least one primary table is searched for a matching signature to a packet, and a matching signature is found, the at least one secondary table is accessed.

12. The security policy database cache of claim 11 wherein if the selector match is successful flags and SA information are returned to a requesting device.

13. The security policy database cache of claim 1 wherein the at least one primary table is a first one of a plurality of primary tables and the at least one secondary table is a first one of a plurality of secondary tables.

14. The security policy database cache of claim 13 wherein when one of the plurality of primary tables is searched for a matching signature to a packet, and if no matching signature is found, the secondary table for the one of the plurality of primary tables is not accessed.

15. The security policy database cache of claim 14 wherein when one of the plurality of primary tables is searched for a matching signature to a packet, and a matching signature is found, the secondary table for the one of the plurality of primary tables is read and a selector is compared with the selector from the packet.

16. The security policy database cache of claim 14 wherein if the selector match is successful flags and security association (SA) information are returned to a requesting device.

17. A method comprises:

producing a signature of a packet and at least first and second indexes into corresponding first and second primary tables of a security database cache;

reading contents of a bucket from a first one of the primary tables and a bucket from a second one of the primary tables to determine whether either of the buckets have contents that match to the produced signature; and for a match,

determining if a selector in an entry in a secondary table matches a selector of the packet; and if a match

processing according to an operation indicated by the entry.

18. The method of claim 17 wherein processing comprises, processing the packet by reading flags for the packet entry to process the packet according to the flags.

19. The method of claim 17 wherein the cache uses the IP packet selector from a packet and hashing algorithm to produce the signature.

20. The method of claim 17 wherein the actions taken with the packet depend on the value of the flags and include dropping the packet if the flags indicate drop, bypass, and enter a secure network.

21. The method of claim 17 wherein the packets are incoming packets.

22. The method of claim 17 wherein the packets are outgoing packets.

23. The method of claim 17 wherein an entry is added to the security policy database cache.

24. The method of claim 17 wherein if the signatures are exhausted, the method further comprises:

searching a security policy database to locate the proper operation for the packet and to locate the correct security associations (Sas) to apply to the packet; and

inserting the located correct SA as a cache entry into a SPD cache.

25. The method of claim 17 wherein packet processing determines if the signature equals zero, and if zero, the

packet processing sets the signature to another, non-zero value.

26. The method of claim 17 wherein the packet processing repeats until either all the matching signatures are exhausted or a secondary table match is found.

27. A computer program product residing on a computer readable medium for processing a packet comprises instructions to cause at least one processor to:

produce a signature of a packet and first and second indexes into corresponding first and second primary tables of a security database cache;

read contents of a bucket from a first one of the primary tables and a bucket from a second one of the primary tables to determine whether either of the buckets have contents that match to the produced signature; and for a match,

process according to an operation indicated by the entry.

28. The computer program product of claim 27 wherein processing comprises, processing the packet by reading flags for the packet entry to process the packet according to the flags.

29. The computer program product of claim 27 wherein the cache uses the IP packet selector from a packet and hashing to produce the signature.

30. The computer program product of claim 27 wherein the actions taken with the packet depend on the value of the flags and include dropping the packet if the flags indicate drop, bypass, and enter a secure network.

31. The computer program product of claim 27 wherein the packets are incoming packets.

32. The computer program product of claim 27 wherein the packets are outgoing packets.

33. The computer program product of claim 27 wherein an entry is added to the security policy database cache.

34. The computer program product of claim 27 wherein if all of the signatures are exhausted, the computer program product of claim 27 further comprises instructions to:

searching a security policy database to locate the proper operation for the packet and to locate the correct security associations (Sas) to apply to the inbound IPsec packet; and

inserting the located correct SA as a cache entry into a SPD cache.

35. The computer program product of claim 27 wherein packet processing determines if the signature equals zero, and if zero, the packet processing sets the signature to another, non-zero value.

36. The computer program product of claim 27 wherein the packet processing repeats until either all the matching signatures are exhausted or a secondary table match is found.

37. A network forwarding device comprising:

at least one physical interface;

a framer;

a network processor;

security policy database cache to provide data to the network processor when processing packets, the security policy database including:

at least one primary table including signature values that indicate that a packet's SPD information may be in the cache; and

at least one secondary table including cache entries having a selector, flags, SA information and an operation to perform on the corresponding packet for which a cache lookup was made; and

a switch fabric.

38. The device of claim 37 wherein the interface is a media access controller device.

39. The device of claim 37 further comprising SDRAM storing the at least one secondary table.

40. The device of claim 37 further comprising SRAM storing the at least one primary table.

41. The device of claim 37 further comprising local memory to store the at least one primary table.

42. The device of claim 37 further comprising scratchpad memory to store the at least one primary table.